CLAIMS

1. A cryptographic method during which use is made of a random number generator producing random numbers S_i of size N fixed between 0 and W-1, in order to produce a random number R between 0 and a predefined limiter K, characterised in that:

E31: a random variable S_i between 0 and W-1 is produced,

E32: if the random variable S_i is strictly less than a coefficient K_i of the limiter K in base W, then the coefficient R_i of rank i of the random number R is equal to the random variable S_i and then, for any rank J less than i, a random variable S_j between 0 and W-1 is produced and $R_j = S_j$,

E33: otherwise, if the said random variable is greater than the coefficient K_i of rank i of the limiter K in base W, then the said coefficient R_i is determined from the random variable S_i of rank i according to a predetermined function, and then the coefficient R_{i-1} is determined for the random number R of rank i-1 that is immediately lower by repeating steps E31 to E33.

2. A method according to claim 2, during which the following steps are performed:

E1: the limiter K is decomposed in base (W^{p-1}, W^{p-2} ..., W^0) in the form $K=\sum_{i=0}^{p-1} K_i * W^i$, i being a loop index, K_i being a coefficient of the limiter K of rank i between 0 and W-1 and p being the degree of the limiter K,

E2: a Boolean variable f is initialised to TRUE,

E3: the following operations are performed, in a loop indexed by i, i being an integer varying between p-1 and 0:

E31: a random variable S_i between 0 and W0-1 is produced,

E32: if the random variable S_i is strictly less than the coefficient K_i of rank i, then the Boolean variable f is set to FALSE,

E33_1: if the random variable S_i is strictly greater than the coefficient K_i of rank i and the Boolean variable f is TRUE, then the coefficient R_i of rank i is determined from the random variable S_i of rank i according to a predefined function,

E33_2: otherwise $R_i = S_i$

E34: the loop indexed i is decremented,

E4: the random number R is determined by recombination of the random coefficients R_i in base W according to the equation: $R = \sum_{i=0}^{p-1} R_i * W^i$.

3. A method according to claim 2, during which, in order to determine the coefficient R_i of rank i from the random variable S_i of rank i (steps E33_1 and E33_2), the following substeps are performed:

E33_11: if the random variable S_i is strictly greater than the coefficient K_i of the limiter K, then a new random variable S_i is produced,

E33_12: step E33_11 is repeated until the random variable S_i is less than the coefficient K_i of the

limiter K, and then the coefficient R_i is equalised to the random variable S_i.

4. A method according to claim 2, during which the coefficient R_i of rank i is chosen (steps E33-1 and E33_2) equal to the part of the random variable S_i, the part less than the coefficient K_i, the said part corresponding to a limited number of bits of the variable S_i.

5. A method according to claim 2, during which, in order to determine the coefficient R_i of rank i from the random variable S_i of rank i (step E33), the random variable S_i is reduced modulo K_i+1, the result of the reduction being the coefficient sought.

6. A method according to one of claims 1 to 5, during which, in order to determine the coefficient R_i of rank i from the random variable S_i of rank i (step E33), steps E1 to E4 are executed using a base (β^{q-1}, ..., β^0) as the calculation base, β being an integer strictly less than W and q being the degree of k in case β.

7. A method according to claim 6, in which step E33 is broken down into the following substeps:

E33_41: the coefficient K_i of rank i of the limiter K in base (β^{q-1}, ..., β^0) in the form $K_1 = \sum_{j=0}^{q-1} (K_i)_j * \beta^j$, j being a loop index, $(K_i)_j$ being a number between 0 and β-1 and q being a degree of the coefficient K_i, is decomposed,

E33_42: a second Boolean variable g is initialised to TRUE,

E33_43: the following operations are performed, in a loop indexed by j varying between q-1 and 0:

E33_431: a random variable $(S_i)_j$ between 0 and β-1 is produced,

E33_432: if the random variable $(S_i)_j$ is strictly less than the coefficient $(K_i)_j$, then the second Boolean variable g is set to FALSE,

E33_4331: if the random variable $(S_i)_j$ is strictly greater than the coefficient $(K_i)_j$ and the second Boolean variable g is TRUE, then a coefficient $(R_i)_j$ is determined from the random variable $(S_i)_j$ according to a predefined function,

E33_4332: otherwise, $(R_i)_j = (S_i)_j$

E33_434: the loop indexed j is decremented,

E33_44: the random number R_i is determined by recombination of the random coefficients $(R_i)_j$ in base β according to the equation: $R_1 = \sum_{j=0}^{q-1} (R_i)_j * \beta^j$.

8. An electronic component comprising a generator of random numbers of size N, calculation circuits performing in particular a comparison, a truncation and/or a modular reduction on numbers of no more than N bits, and a means of controlling the random number generator and calculation circuits, the said control means being adapted for implementing a method according to one of claims 1 to 7.

9. A chip card comprising an electronic component according to the preceding claim.